

Problem beim Erstellen einer Firmware und SSDT für Thunderbolt 3 AIC

Beitrag von „schrup21“ vom 10. Juni 2025, 08:08

Also vorweg: sichere und verifiziere lieber 3x deine Firmware, damit du zurück kannst

Am Begin ist ein Pointer, der auf den Anfang der Firmware zeigt:



```
000000 00400000 00000800 00000000 00000000 FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF @ .....
000020 FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF .....
```

das ist die FW Sektion (darunter btw. DROM):


```

Move selection to 0x4035 Move
003F40 FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF
003F80 FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF
003FA0 FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF
003FC0 FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF
003FE0 FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF
004000 3B017F10 1CD315B0 00004100 ADAD0035 0611BF05 50505353 85042D84 80F0A023
004020 24002400 24002400 2E002E00 2EC02E00 00000000 27272727 D3150033 80010000
004040 052D28AD 2D28AAAA 04282804 955679A6 03404120 A0E4C61B 39811B81 E4E48000
004060 20403000 03150000 01000000 41505020 45402020 C6100000 003FA703 BB000000
004080 00100000 000004E2 00300039 00000205 02100100 0000E0C2 000C2200 00000400
0040A0 1A105533 11222D2F 330A0000 4E44A000 00010F05 00001A30 95100000 00FF0310
0040C0 00001E10 0A003710 0C000010 0E001810 10000490 00000000 00000010 14004800
0040E0 00000010 18000500 00000002 20F00D2 41313F63 F40B7174 DAB0100 1F1F0807
004100 0C000111 10131200 00001212 12121002 00000000 00000009 0A000000 00000000
004120 00000000 00000000 00FF0000 00000000 00000000 00000000 50000000 00030000
004140 001E3028 00FFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF
004160 FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF
004180 FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF
0041A0 FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF
0041C0 FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF
0041E0 FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF
004200 44524F4D 20202020 FFFFFFFF FFFFFFFF 75000000 00000049 1205F0 40016A00
004220 43180100 65260881 80020000 00000882 90018A00 00000883 8004A001 00000884
004240 90030001 000002C5 00862001 00040000 00000003 8780558 50000005 89500000
004260 05A50000 00058050 00000001 4153526F 63600014 02546875 6E646572 626F6C74
004280 20332041 49430000 00000000 00000000 00000000 00000000 00000000 00000000
0042A0 00000000 000000FF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF
003F00 FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF
003F20 FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF
003F40 FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF
003F60 FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF
003F80 FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF
003FA0 FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF
003FC0 FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF
003FE0 FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF
004000 3B017F10 1CD315B0 00004100 ADAD0035 0611BF05 50505353 85042D84 80F0A023
004020 24002400 24002400 2E002E00 2EC02E00 00000000 27272727 D3150033 80010000
004040 052D28AD 2D28AAAA 04282804 955679A6 03404120 A0E4C61B 39811B81 E4E48000
004060 20403000 03150000 01000000 41505020 45402020 C6100000 003FA703 BB000000
004080 00100000 000004E2 00300039 00000205 02100100 0000E0C2 000C2200 00000400
0040A0 1A105533 11222D2F 330A0000 4E44A000 00010F05 00001A30 95100000 00FF0310
0040C0 00001E10 0A003710 0C000010 0E001810 10000490 00000000 00000010 14004800
0040E0 00000010 18000500 00000002 20F00D2 41313F63 F40B7174 DAB0100 1F1F0807
004100 0C000111 10131200 00001212 12121002 00000000 00000009 0A000000 00000000
004120 00000000 00000000 00FF0000 00000000 00000000 00000000 50000000 00030000
004140 001E3028 00FFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF
004160 FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF
004180 FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF
0041A0 FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF
0041C0 FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF
0041E0 FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF
004200 44524F4D 20202020 FFFFFFFF FFFFFFFF 6C000000 00001001 00062628 35010000
004220 01000C00 0100FF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF
004240 FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF
004260 FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF
004280 FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF
0042A0 FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF

```

Theoretisch könnte auch OSY's Weg über den Ti Power Controller funktionieren, dabei werden die Offsets über den Ti überschrieben - allerdings patcht der 9 Abschnitte (k.A. warum, einige sind aber im DROM Abschnitt, den wir ja über die SSDT patchen) inkl. 0x35 und 0x81 (ist in seiner Plist Dezimal angegeben). Ich glaube der 1. Patch ist nur um den Beginn der FW zu finden...

<https://osy.gitbook.io/hac-min.../thunderbolt-3-fix-part-3>

<https://github.com/osy/Thunder...s Canyon Apple Mode.plist>

```

<dict>
  <key>Offset</key>
  <integer>0</integer>
  <key>Original</key>
  <data>0wE=</data>
  <key>Replace</key>
  <data>0wE=</data>
</dict>
<dict>
  <key>Offset</key>
  <integer>53</integer>
  <key>Original</key>
  <data>Jyc=</data>
  <key>Replace</key>
  <data>Nzc=</data>
</dict>
<dict>
  <key>Offset</key>
  <integer>129</integer>
  <key>Original</key>
  <data>oA=</data>
  <key>Replace</key>
  <data>IA=</data>
</dict>

```

Mit Titan Ridge geht das aber nicht soweit ich weiß, daher weiß ich da nicht mehr... Hat aber den charmanten Vorteil, dass man auf Apple und zurück auf Default patchen kann, ohne den Chip komplett flashen zu müssen.

Das mit den 3 Bytes hab ich zuerst im "Thunderbolt 4" Thread gelesen (Tony verlinke ich lieber nicht - auf Insanely nicht erlaubt, k.A. wie das hier gesehen wird). Elias64Fr hat da von den 3

Bytes geschrieben, gleich TB3...